

Risiko Online-Banking

Kunden fallen auf Rücküberweisungstrojaner herein: kein Schadenersatz von der Sparkasse

Wer sich für Online-Banking anmeldet, muss vorher die einschlägigen Geschäftsbedingungen seines Kreditinstituts unterschreiben. Darin verpflichten sich die Kunden auch, die Sicherheitshinweise zu beachten. Mitteilungen auf der Online-Banking-Seite ihrer Bank oder ihrer Sparkasse sollten die Kunden daher aufmerksam lesen, wie folgender Fall zeigt.

Eine Sparkasse warnte dort eindringlich vor Banking-Trojanern: "Unter dem Vorwand, das Konto zu entsperren oder eine Rücküberweisung tätigen zu müssen", forderten diese Schadprogramme den Kunden dazu auf, eine TAN zu generieren und einzugeben. (Beim TAN-Verfahren wird für jede Überweisung mit einem TAN-Generator eine eigene TAN (Transaktionsnummer) erzeugt.)

Diese TAN werde für eine betrügerische Überweisung generiert. Wenn beim Online-Banking etwas ungewöhnlich ablaufe, sollten die Kunden den Vorgang abbrechen und mit ihr Kontakt aufnehmen, empfahl die Sparkasse.

Ein Ehepaar fiel auf so einen Trojaner herein: Als der Mann im Internet den Online-Banking-Account aufrief, erschien ein Pop-up-Fenster, das sich nicht wegklicken ließ. Es enthielt einen Text, der ihn erschreckte: Der Online-Banking-Account werde gesperrt, stand da, wenn die Kontoinhaber nicht eine fehlgeleitete Überweisung in Höhe von 2.773 Euro auf das Konto von Herrn R zurück-überweisen.

Eine entsprechende Gutschrift sei tatsächlich in den Umsätzen ihres Girokontos aufgetaucht, erklärten die Eheleute später. Diese Meldung sei aber verschwunden, als sie mit einer TAN 2.773 Euro auf das Konto von Herrn R überwiesen. Danach ließ das Ehepaar sein Online-Banking-Konto sperren, doch das Geld war natürlich weg.

Die Bank ist nicht verpflichtet, den Betrag zu ersetzen, urteilte das Amtsgericht Köln (119 C 143/13). Trotz der Warnung der Sparkasse hätten die Kunden das Online-Überweisungsformular ausgefüllt und per TAN-Eingabe den Betrag freigegeben. Dabei habe das Kreditinstitut vor Banking-Trojanern gewarnt, die aktiv würden, wenn Kunden ihre Online-Banking-Seite aufriefen.

Ausdrücklich habe die Sparkasse darauf hingewiesen, dass es vom gewöhnlichen Einloggen beim Online-Banking-Account abweiche, wenn sich ein Pop-up-Fenster öffne. Werde in diesem Fenster eine Kontosperrung angedroht, wenn nicht eine bestimmte Finanztransaktion stattfinde, liege der Gedanke an eine Phishing-Attacke nahe. Daraufhin hätte das Ehepaar den Vorgang beenden und der Bank melden müssen.

© Der Juristische Pressedienst Gritschneder UG ist Inhaber sämtlicher Inhalte und Nutzungsrechte. Diese sind urheberrechtlich geschützt. Auf die Nutzungsbedingungen wird verwiesen.